Tax Practitioner Guide to Business Identity Theft

Guidance for business clients who may be victims of identity theft

When your client becomes a victim of identity theft, it can be very frustrating and time-consuming to resolve. The following information can help you help your client navigate the process of protecting their business information from further misuse.

What is business identity theft?

Business identity theft happens when someone creates, uses or attempts to use the identifying information of a business, without authority, to obtain tax benefits. Business identity thieves file fraudulent business returns to receive refundable business credits or to perpetuate individual identity theft.

How do I know if my client's business information has been affected?

Sometimes the identity theft incident is related to tax administration and sometimes it's not. The incident may surface in different ways.

Identity theft related to tax administration:

Business identity theft is more complex than individual identity theft. Many of the same indicators that signify simple filing or processing errors also hint at business identity theft. While on the surface these occurrences may appear to indicate business identity theft, they may also stem from something as simple as transposed numbers.

- Your client receives IRS notices about fictitious employees.
- Your client notices activity related to or receives IRS notices regarding a defunct, closed or dormant business after all account balances have been paid.
- Your client's return is accepted as an amended return, but the taxpayer has not filed a return for that year.

If these things occur, the IRS and the taxpayer will need to do some research before determining the incident is a result of identity theft.

Identity theft not related to tax administration should be reported to the Federal Trade Commission. Find additional information on how to identify identity theft on the FTC website at http://www.consumer.ftc.gov/topics/privacy-identity

Clients may be victims of identity theft not related to tax administration if they:

- receive bills for business lines of credit or credit cards they do not have.
- notice that a credit report indicates credit or other open accounts they did not authorize.
- see unexplained bank account withdrawals.
- don't get their bills or other mail.
- find unfamiliar accounts or charges on their credit report.
- get a notice that information was compromised by a data breach at a company where they do business or have an account.

What protective actions should my clients take if their business information has been compromised?

- Respond immediately to any notices from the IRS. If they believe someone fraudulently used their Employer Identification Number, notify the IRS immediately using the contact information on the notice or letter.
- File a police report with the local police department.
- Carefully review and reconcile account statements as soon as they receive them.
- Regularly review business registration information online (for all active and closed businesses).
- Monitor credit reports for suspicious activity every 12 months.
- Place a fraud alert on credit reports by contacting any one of the four nationwide credit reporting companies:

Dun & Bradstreet	800-234-3867	www.smallbusiness.dnb.com
Equifax	800-525-6285	www.equifax.com
Experian	888-397-3742	www.experian.com
Trans Union	800-916-8800	www.transunion.com

- Close any accounts that have been tampered with or opened without their permission.
- File a complaint with the Federal Trade Commission.
- Update virus, malware, and other security software programs on their computers.
- Remain vigilant and be alert for suspicious or unusual activity.